

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

ALONSO GUTIERREZ, on behalf of himself
and all similarly situated individuals,

Plaintiff,

v.

RECOGNITION SYSTEMS, INC. and
INGERSOLL RAND, INC.

Defendants.

Case No.: 9:24-3999

CLASS ACTION COMPLAINT

Plaintiff Alonso Gutierrez (“Plaintiff”) brings this Class Action Complaint against Recognition Systems, Inc. (“RSI”) and Ingersoll Rand, Inc. (“IR”) (collectively Defendants) for violations of the Illinois Biometric Information Privacy Act (“BIPA”).

SUMMARY OF CLAIMS

1. BIPA defines a “biometric identifier” as any personal feature that is unique to an individual, including fingerprints and hand geometry. 740 ILCS 14/10.
2. “Biometric information” is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS 14/10. Collectively, biometric identifiers and biometric information are known as “biometrics.”
3. Under BIPA, biometric information is treated and regulated the same as biometric identifiers.
4. Defendants are manufacturers and vendors of, among other things, time and attendance solutions to employers, and provides its customers with biometrically-enabled devices and technology in order to perform workforce management services on their behalf, such as timekeeping and work-scheduling services.

5. Defendants' technology captures the biometric identifiers of its clients' employees and transmits information and data derived from those biometric identifiers directly to Defendants' cloud-based time and attendance systems. This information that Defendants receive and possess is generated and derived from the scanning of Plaintiff's and other Class members' biometric identifiers. Thus, Defendants obtain and possess biometric information.

6. BIPA provides, *inter alia*, that private entities, such as Defendants, may not collect, capture, purchase, or otherwise obtain an individual's biometric identifiers, such as fingerprints and hand scans, or any biometric information, including any data regardless of the manner from which it was converted, or is converted or stored, unless they first:

- (a) inform that person in writing that biometric identifiers or biometric information will be collected or stored;
- (b) inform that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used; and
- (c) receive a written release from the person for the collection of their biometric identifiers or biometric information. 740 ILCS 14/15(b)(1)-(3).

7. BIPA also requires private entities in possession of biometric information to develop a publicly-available written policy outlining the storage and destruction policies of such biometric identifiers, and/or any biometric information derived from such identifiers. 740 ILCS 14/15(a)

8. Finally, private entities are prohibited from profiting from an individual's biometric identifiers or biometric information. 740 ILCS 14/15(c).

9. BIPA recognizes that “biometrics are unlike other unique identifiers that are used to access finances or other sensitive information,” 740 ILCS 14/5, and therefore require special treatment compared to other types of personal information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. “Biometrics, however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions.” 740 ILCS 14/5.

10. Plaintiff brings this action for statutory damages and other remedies as a result of Defendants’ conduct in violating his biometric privacy rights under BIPA.

11. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendants to comply with BIPA, as well as an award of statutory damages to the Class members and monetary damages to be determined at trial, together with costs and reasonable attorneys’ fees.

PARTIES

12. Plaintiff is a natural person and citizen of the State of Illinois.

13. Defendants are vendors of cloud-based timekeeping and attendance tracking products and services. Defendants sell such products and services to clients located in Illinois.

14. Defendant RSI is a New York corporation with its headquarters in Port Washington, New York.

15. Defendant IR is incorporated in Delaware.

16. IR is a global provider of industrial solutions, with its headquarters in Davidson, North Carolina.

17. RSI is a wholly-owned subsidiary of IR. <https://www.sec.gov/Archives/edgar/data/1466258/000119312510043035/dex21.htm> (last visited May 30, 2024).

18. RSI has operated as the biometric component of IR's Security & Safety Group's Electronic Access Control Division.

JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendants because, during the relevant time period, Defendants did business in this judicial district, were registered to do business in New York.

20. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because Plaintiff and Defendants are citizens of different states, there are estimated to be thousands of potential class members, and over \$5,000,000 is in controversy.

21. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b)(1) and (2).

DEFENDANTS' BIOMETRIC DEVICES

22. IR and RSI have developed a hand geometry scanner used for biometric timekeeping which is referred to as HandPunch.

23. HandPunch requires users to scan their fingerprints and/or hand geometry for timekeeping purposes. The HandPunch device advertises that it takes over 90 distinct measurements of an employee's hand. These measurements include length, width, thickness, and surface area of the hand. Notably, Defendants advertise its HandPunch as collecting biometric information.

24. Examples of biometric devices manufactured and sold by Defendants are below:





25. Defendants market and sell its biometric time clocks to employers in Illinois.

26. Unlike key fobs, identification numbers, or swipe cards – which can be changed or replaced if stolen or compromised – fingerprints and/or hand geometry biometrics are unique, permanent biometric identifiers associated with each employee. This exposes employees who are

required to use Defendants' devices as a condition of their employment to serious and irreversible privacy risks.

27. During the relevant time period, Defendants sent one or more biometric devices into the State of Illinois with the knowledge that its device would be capturing, obtaining, using, and/or collecting biometric information from Illinois residents.

28. When an employee first begins work at an Illinois company that uses one of Defendants' biometric devices, the employee is required to have his/her fingerprint and/or hand geometry scanned into the HandPunch biometric device in order to enroll him/her in the Defendants' database.

29. Defendants then store the biometric information and/or identifiers of Illinois residents in its database so that Illinois employers can access the biometric information to use this information for payroll and attendance confirmation.

30. When an Illinois resident employed by a company in Illinois scans its biometric information into Defendants' biometric device Defendants become aware that it is in the possession of Illinois residents' biometric information.

PLAINTIFF'S BIOMETRIC INFORMATION

31. Plaintiff was employed by a third party in the State of Illinois at McFarlane Douglass, from May 4, 2016, through November 6, 2023.

32. As a condition of his employment by McFarlane Douglass, Plaintiff was required to scan his fingerprints and/or hand geometry on Defendants' biometric device each day of work to clock-in and clock-out of work.

33. When beginning his first day of work Plaintiff was required to scan his fingerprints and/or geometry on Defendants' biometric device so that his biometric information could be kept in Defendants' database. An image of the HandPunch device Plaintiff was required to use is below:



34. Plaintiff scanned his fingerprints and/or hand geometry on Defendants' device while he was physically present and working in the State of Illinois.

35. Defendants thereafter collected and stored Plaintiff's biometric data in their database(s) immediately after it was captured in the State of Illinois.

36. Plaintiff was required to scan his fingerprints and/or hand geometry on Defendants' device each time he clocked in and out for work including each time he clocked out for a meal break and then clocked back in when returning from a meal break.

37. During his employment period Plaintiff scanned his fingerprints and/or hand geometry on Defendants' biometric device hundreds of times.

38. During the 5 years preceding the filing of this lawsuit, Defendants collected fingerprints and/or hand geometry scans from hundreds (if not thousands) of other Illinois residents through its reader/scanner to help its business clients in Illinois verify employees and document the number of hours worked at its clients' locations in Illinois. Defendants collected the biometric information from individuals in Illinois because Plaintiff and other similarly situated individuals, were required to scan their fingerprints and/or hand geometry on a daily basis by using their fingerprints and/or hand geometry with Defendants' scanner so that the employer could track the number of hours worked.

39. Accordingly, Defendants collected, stored, used, or otherwise obtained biometric information from Plaintiff and similarly situated individuals.

40. Defendants then stored and collected Plaintiff and similarly situated individuals' fingerprints and/or hand geometry in its database.

41. Plaintiff's fingerprints and/or hand geometry are considered "biometric information" as that term is defined under BIPA.

42. Defendants failed to obtain express written consent from Plaintiff when it used biometric technology in connection with its time-keeping system and prior to obtaining, collecting, or possessing Plaintiff's biometric information.

43. The actions of Defendants violate the Plaintiff's statutory privacy rights under BIPA.

44. Defendants never informed Plaintiff of the specific purpose and length of time for which his biometric identifiers or information would be collected, stored, and used, nor did Defendants obtain a written consent or release from Plaintiff.

45. Defendants did not have written, publicly available policies identifying their retention schedules or guidelines for permanently destroying users' biometric identifiers or information.

46. Plaintiff has been required to retain the undersigned counsel to protect and enforce his rights under BIPA and is therefore entitled to recover reasonable attorney's fees and costs.

CLASS ALLEGATIONS

47. Plaintiff seeks to represent a class of Illinois residents who had one or more of their fingerprints and/or hand geometry scans captured, collected, or otherwise obtained by Defendants in Illinois between June 3, 2019 and the present ("the Class").

48. Plaintiff and the Class are similar to one another because they were all subject to the same allegedly illegal practices: Defendants capturing, collecting or otherwise obtaining scans of their fingerprints and/or hand geometry without adhering to the requirements of the Biometric Information Privacy Act.

49. The Class includes more than 50 members.

50. As a result, the Class is so numerous that joining of all class members in one lawsuit is not practical.

51. The issues involved in this lawsuit present common questions of law and fact, including: whether Defendants captured, collected, or otherwise obtained fingerprints and/or hand geometry from the Class; whether the fingerprints and/or hand geometry scan data Defendants captured qualifies as "biometric identifiers" under the Biometric Information Privacy Act; and

whether Defendants made written disclosures and obtained informed written consent before capturing, collecting, or otherwise obtaining scans of fingerprints and/or hand geometry from the Class.

52. These common questions of law and fact predominate over variations that may exist between members of the Class, if any.

53. Plaintiff, the members of the Class, and Defendants have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

54. If individual actions were required to be brought by each member of the Class injured or affected, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendants.

55. Accordingly, a class action is an appropriate method for the fair and efficient adjudication of this lawsuit and distribution of the common fund to which the Class is entitled.

56. The books and records of Defendants are material to Plaintiff's case as they disclose how Defendants captured, collected, or otherwise obtained fingerprints and/or hand geometry from Plaintiff and the Class and what information Defendants provided Plaintiff and the Class about its capture, collection, and use of their biometric identifiers.

57. Plaintiff and his counsel will fairly and adequately protect the interests of the Class.

58. Plaintiff retained counsel experienced in complex class action litigation, including class action litigation under the Biometric Information Privacy Act.

COUNT I
Violation of the Biometric Information Privacy Act (740 ILCS 14/15(b))
(Class Action)

59. Plaintiff realleges and incorporates the previous allegations of this Complaint.

60. Defendants are "private entit[ies]" under the Biometric Information Privacy Act. 740 ILCS 14/10.

61. Plaintiff's and the Class's fingerprints and/or hand geometry scans qualify as "biometric identifier[s]" as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

62. Defendants have "biometric information" from Plaintiff and the Class through their acquisition and retention of information based on Plaintiff's and the Class's fingerprint and/or hand geometry scans.

63. Defendants violated the Biometric Information Privacy Act by capturing or collecting Plaintiff's and the Class's fingerprints and/or hand geometry scans and personal identifying information based on their fingerprints and/or hand geometry scans without first informing them in writing that Defendants were doing so.

64. Defendants violated the Biometric Information Privacy Act by capturing or collecting Plaintiff's and the Class's fingerprints and/or hand geometry scans and personal identifying information based on their fingerprints and/or hand geometry scans without first informing them in writing of the purpose of Defendants doing so and the length of time Defendants would store and use Plaintiff's and the Class's biometric identifiers and/or biometric information.

65. Defendants violated the Biometric Information Privacy Act by capturing or collecting Plaintiff's and the Class's fingerprints and/or hand geometry scans and personal identifying information based on their fingerprints and/or hand geometry scans without first obtaining their written consent or other release authorizing Defendants to capture or collect Plaintiff's and the Class's biometric identifiers and/or biometric information.

66. Unlike other companies, Defendants failed to take notice and follow the requirements of the Biometric Information Privacy Act even though the law was enacted in 2008 and numerous articles and court filings about the law's requirements were published before Defendants committed the legal violations alleged in this Complaint.

WHEREFORE, Plaintiff and the Class pray for a judgment against Defendants as follows:

- A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and each member of the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);
- B. Enjoining Defendants from committing further violations of the Biometric Information Privacy Act as authorized by 740 ILCS 14/20(4);
- C. Awarding Plaintiff's reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and
- D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

COUNT II

Violation of the Biometric Information Privacy Act (740 ILCS 14/15(a)) (Class Action)

67. Plaintiff realleges and incorporates the previous allegations of this Complaint.

68. Defendants are "private entit[ies]" under the Biometric Information Privacy Act. 740 ILCS 14/10.

69. Plaintiff's and the Class's fingerprints and/or hand geometry scans qualify as "biometric identifier[s]" as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

70. Defendants have "biometric information" from Plaintiff and the Class through its acquisition and retention of information based on Plaintiff's and the Class's fingerprints and/or hand geometry scans.

71. Defendants violated the Biometric Information Privacy Act by possessing Plaintiff's and the Class's fingerprints and/or hand geometry scans and personal identifying information based on their fingerprints and/or hand geometry scans without creating and following a written policy, made available to the public, establishing a retention schedule and destruction guidelines for its possession of biometric information derived from Plaintiff's and the Class's

fingerprints and/or hand geometry scans.

72. Unlike other Illinois companies, Defendants failed to take notice and follow the requirements of the Biometric Information Privacy Act even though the law was enacted in 2008 and numerous articles and court filings about the law's requirements were published before Defendants committed the legal violations alleged in this Complaint.

73. As a result, Defendants' violations of the Biometric Information Privacy Act were reckless or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against Defendants as follows:

- A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and each member of the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);
- B. Enjoining Defendants from committing further violations of the Biometric Information Privacy Act as authorized by 740 ILCS 14/20(4);
- C. Awarding Plaintiff his reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and
- D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

Dated: June 3, 2024

Respectfully submitted,

/s/ Jordan Richards

One of the Attorneys for
Plaintiff and the proposed Class

Douglas M. Werman- IL. Bar #- 6204740 dberman@flsalaw.com Maureen A. Salas- IL. Bar #- 6289000 msalas@flsalaw.com Werman Salas P.C. 77 W. Washington St., Suite 1402 Chicago, IL 60602 Ph: (312) 419-1008	Jordan Richards (NY Bar No. 5859095) jordan@jordanrichardspc.com Jordan Richards PLLC 1800 SE 10th Ave. Suite 205 Fort Lauderdale, Florida 33316 Ph: (954) 871-0050
---	---

